Unit-5 WEB SECURITY

1. Indicate the security of threats faced while using web.

The security threats can be classified into two types: Active attacks, Passive attacks

Active attacks: Acts as an authenticate user and alters the message when message transfers from client and server.

Passive attacks: Intruders on network who gains access to information which transfers from client to server.

Another way to classify the security threats in terms of location:

Web browser

Web server

Network traffic between browser and server

2. List the parameters of SSL session state.

There are 6 parameters in SSL Session State:

1)Session Identifier: It is a sequence chosen by server to identify an active or resumable session state.

2)Peer Certificate: It is an X509.v.3 certificate of the peer. And also this element can be null.

3) Compression Method: It is algorithm used to compress data prior to encryption.

4) Cipher Spec: It indicates bulk data encryption and hash algorithm used for MAC calculation.

5) Master secret: It's a 48 byte secrete code id shared between the client and server.

6) Is resumable: It's a flag indicating whether the session can be used to initiate new connection.

3. List the parameters of SSL Connection state.

There are 7 parameters

1) Server and Client Random: The byte sequence chosen by the server and client for each connection.

2) Server write MAC secret: It is a secret key used in MAC operations on data sent by the server.

3) Client write MAC secret: It is secret key used for encrypted data sent by the client.

4) Server write key: It's a secrete encryption key for data encrypted by server and decrypted by client.

5) Client write key: It's a secrete encryption key for data encrypted by client and decrypted by server.

4. List the services provided by SSL record protocol.

The SSL record protocol provides 2 different services for SSL connections. They are:

1) Confidentiality: The Handshake protocol defines shared secret key, which should be confidential.

   Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

2) Message Integrity: The Handshake protocol defines shared secret key, which is used to form MAC.

   Message Integrity describes the concept of ensuring that data has not been modified in transit.

5. Write a note on S-HTTP.

This protocol provides secure or safe exchange of files on World Wide Web.

Each S-HTTP file is either encrypted or it contains digital certificate or both.

S-HTTP allows its clients to send an authentication certificate to authenticate the end-users.

S-HTTP uses CMS (cryptographic message Syntax Algorithm) to secure each individual messages.

With S-HTTP, messages can be encrypted on per transaction basis using symmetric session keys.

It provides mechanisms for authentication and signature of messages.

It provides support for implementing different kinds of cryptographic algorithms and key management systems.

6. Write a note on Secure Electronic Transaction (SET).

SET is a system for ensuring the security of **Financial Transactions** on the **Internet.**

SET was a communication protocol standard for securing credit card, visa cards

SET is not a payment system, it consists of group of protocols and formats which enables secure transactions.

Transaction is conducted and gets verified with a combination of Digital certificates and Digital Signatures among purchaser and seller which provides privacy and confidentiality.

SET makes use of: Secure Socket Layer(SSL)

Microsoft's Secure Transaction Technology(STT)

Secure Hypertext Transport Protocol(S-HTTP)

7. Explain the client/server architecture of web.

- Client / Server Architecture is a computer network i.e., group of two or more computers interconnected to share program, data and software / hardware resources.
- Client / Server Architecture is defined as a computing model in which a high configured computer termed as **Server**, delivers and manages most of the resources and services to be utilized by **Client**.
- Client server architecture consists of one or more computers called **Clients** connected to a central high end computer called **Server.** Client server architecture shares computing resources.
- This architecture works when client computer sends a resource/process request to server over the network, which in turn the server delivers requested service back to client.
- Server can manage several clients simultaneously. And also single client can connect to several servers at a time for different services.
- 4.The Internet is a common connection in which computers can communicate using common addressing mechanism with TCP/IP connection.
- 5. Important characteristics of this architecture is Scalability. Scalability refers to adding or removing clients and migrating to larger and faster servers.
- 6. The front end of this architecture interact with end users and at the back end it interacts with shared resources such as printers, databases, processors.

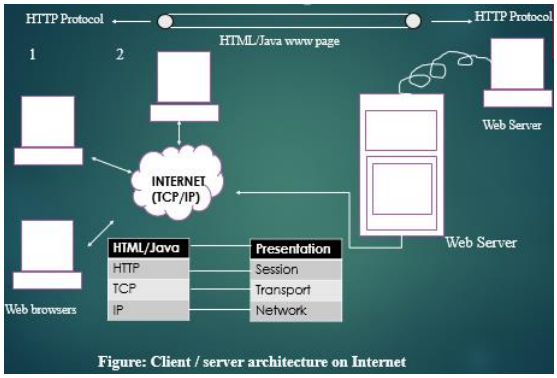


Figure: Client / server architecture on Internet

8. Describe web traffic security approaches.

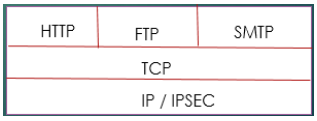
There are many number of approaches exit to provide web security but all of these are similar in the services they provide**.**

3 types of approaches are:

1. At Network level: IP/IPSEC

In this approach IPSEC has filtering capacity such that selected traffic need to incur the process.

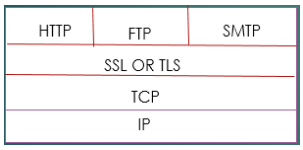
It is transparent to end –users



2. At Transport level: SSL or TLS

IN this approach the application is embedded together in specific application itself. Explorer and browser are embedded with SSL and TLS.

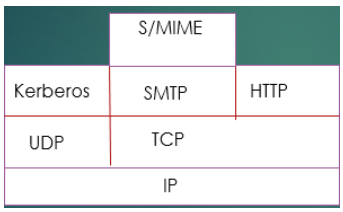
It is transparent to the users.



3. **At Application level: S/MIME, Kerberos**

The application specific security services are embedded together within particular application.

Services can be tailored to specific needs of given application.



9. Explain the importance of SSL/TLS for secure web services.

- It is designed to make use of TCP in order to provide a reliable end – to – end secure web services.
- It is not a single protocol layer, it has 2 different layers of protocol stacked over IP and TCP.

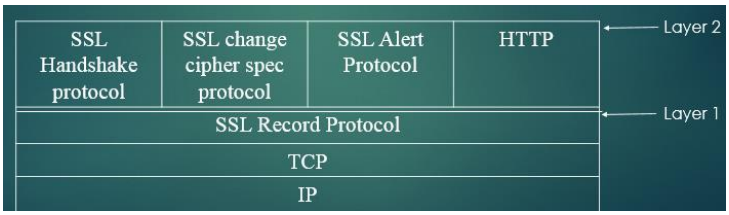


Fig: SSL protocol Stack

- In the first layer SSL RECORD PROTOCOL provides basic security services to higher layer (i.e., layer 2) protocol.
- HTTP (Hyper Text Transfer Protocol) provides transfer services for Web / client –server interaction.
- SSL Handshake Protocol, SSL Change Cipher Spec Protocol and SSL Alert Protocols are used in the management of SSL exchanges.

9. Explain the parameters of SSL session and SSL connection states.

Refer Answers of Question number 2 & 3

10. Describe SSL record protocol with a neat diagram

- SSL record protocol takes an application message to be transmitted. It fragments the application data into manageable blocks.
- It compresses the data and applies a MAC (Message Authentication Code) and performs encryption.
- At the end it adds a header (SSL record header) and transmits the encrypted data to the receiver.
- The received data in turn decrypted, verified, decompressed and reassembled before being delivered to higher –level users.

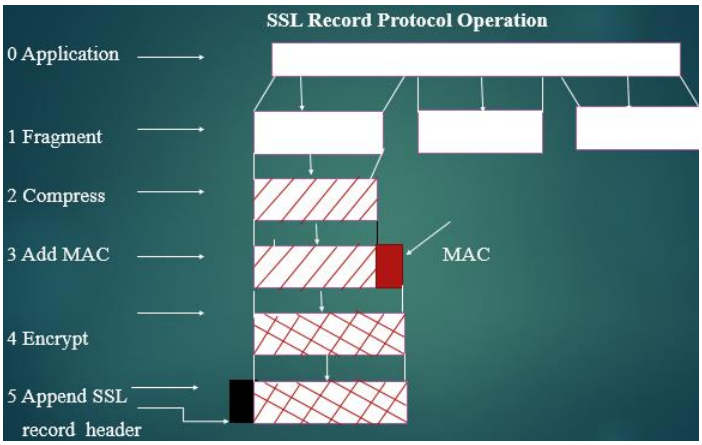
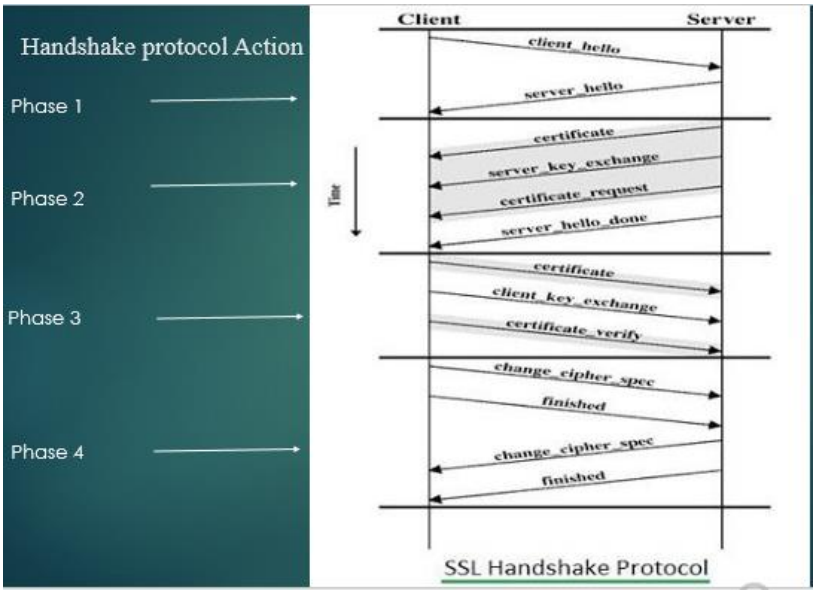


Fig: SSL record protocol

11. Explain SSL handshake protocol

- SSL handshake protocol is used before any application data is transmitted.
- Handshake protocol consists of a series of messages exchanged by client and server.
- This protocol permits both client and server to authenticate each other and to perform encryption, MAC and cryptographic keys to protect data sent in SSL record.
- **Handshake protocol works in 4 phases**:
- **Phase 1:** Hand shaking initiated by client. Establish security connection including protocol version, Session ID, Cipher suit, compression method and initial random numbers.
- **Phase 2:** Server may send certificate, key exchange and request certificate, at the end hello message phase.
- **Phase 3:** Client sends certificate if requested. Client sends key exchange and certificate verification.

- **Phase 4:** Change cipher suit and finish handshake protocol.



12. Explain the flow of transaction in SET with a diagram.

- Both the card holder and merchant should register with Certificate Authority before they can buy or sale on the Internet.
- Once registration is done: card holder and merchant can start transaction as per the 9 basic steps of SET transaction flow.
- To follow these 9 steps of SET, customer must contain a SET enabled browser such as NETSCAPE navigator or Microsoft Internet Explorer. Similarly, merchant should contain SET enabled server.

Step 1	**Customer perform website browsing and determine as what to purchase**
Step 2	Customer submits purchase order and payment details in 2 parts
	a) Purchase order – This is for merchant
	b) Card details – This is for merchant's bank
Step 3	Merchant forwards card details to his respective bank
Step 4	Merchant's bank verifies with issuer for payment address
Step 5	Issuer sends Authorization to merchants' bank
Step 6	Merchants bank in turn sends authorization to merchant
Step 7	Merchant process the order and sends confirmation to customer
Step 8	Merchant captures the transaction from their bank
Step 9	Issuer prints credit card bill to customer

13. Describe the SET components and their relationships

SET system includes the following participants:

Card holder: Customer or purchaser who interact with merchants. Authorized holder of card**.**

Issuer: This is a financial institution; such as bank that provides the card holder with payment card.

Payment Gateway: This is a third party that process merchant payment messages.

Merchant: A person or an organization that has goods or services.

Acquire: This is also a financial institution that establishes an account with a merchant and possess payment card authorization.

Certificate Authentication: This is an entity that issue public key certificates for card holders, merchants.